凌力 编著

不是“预言书”
不是“编程书”
不是“投资书”

层层解构区块链
全面剖析底层细节
深度分析技术演进
细致解析应用场景

清华大学出版社

解构区块链

DECONSTRUCTION OF BLOCKCHAIN

凌　力 编著

清华大学出版社
北京

内 容 简 介

说到区块链，有人好奇地问："什么是挖矿，怎么记账？"也有人想弄清如何实现共识、怎样构建智能合约，还有人困惑于应用与区块链是否能够对接。本书将从区块链底层技术细节开始来逐一回答这些问题。首先，系统性剖析区块链技术的原理和本质，从其产生背景、基本概念出发，深入浅出地解析区块链结构、核心算法、运行机制及其支撑技术；其次，通过诠释区块链技术特征、优势与弱点，进一步分析技术演进、典型应用。

图书在版编目(CIP)数据

解构区块链/凌力编著. —北京：清华大学出版社，2019
ISBN 978-7-302-52058-0

Ⅰ. ①解…　Ⅱ. ①凌…　Ⅲ. ①电子商务－支付方式－研究　Ⅳ. ①F713.36

中国版本图书馆 CIP 数据核字(2019)第 009606 号

责任编辑：梁　颖　李　晔
封面设计：常雪影
责任校对：李建庄
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 装 者：北京嘉实印刷有限公司
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　　张**：19　　**字　　数**：323 千字
版　　次：2019 年 7 月第 1 版　　**印　　次**：2019 年 7 月第1次印刷
定　　价：79.00 元

产品编号：080613-01

前言

既然以比特币为代表的虚拟币们虚火升腾、泡沫横溢，监管部门对其严加管束，大多数民众也并不感冒，那么为什么还要学习、研究区块链？

其实这正是笔者写作本书的原因。

区块链技术来源于比特币，但可脱离于比特币。比特币和其他虚拟币存在的问题是由盲目炒币、黑产交易等引起的，当“币”的属性被剥离后，区块链技术就因其创新的思想、独特的结构、灵巧的配置脱颖而出，备受政府、企业及研究者关注和青睐。从不同领域、不同行业的视角来观察区块链技术，似乎都可以找到区块链技术与自身业务的结合点和应用场景，甚至受到启发形成新的业务模式，促成转型升级。

但是，如果缺乏对区块链技术清晰、正确、系统的认识，实际应用就成为无本之木、无源之水，更严重的是可能走偏方向，造成不可挽回的损失。所以本书的唯一目的就是通过解构区块链技术的方方面面，对技术进行深层剖析，不仅知其然，而且知其所以然。当朦朦胧胧的神秘面纱被掀掉后，展现在眼前的将是“高清版”的区块链技术，一些原有的疑惑、误解或偏见自然就会随之烟消云散。

然而本书并不负责解答所有疑问，诸如“我这个项目能否运用区块链技术？怎么用？”等。因此，在区块链技术方面，本书是一本“三不”书。

首先，不是“预言书”。虽然本书不可避免会涉及一些观点和判

断，也有启发性的案例讨论，但并不专注于阐述行情走势、未来趋势、价值衡量、行业预测、社会影响等比较主观的话题，这些都应该是学习者掌握区块链技术原理后自然、自发、自觉的思考。

其次，不是“编程书”。本书确实将深入区块链技术到比特级别构造的程度，据此开发软件是可行的，而且部分算法用代码形式阐述，可更多是为了能清楚说明问题。

最后，不是“投资书”。本书并没有投资分析、指南、路线之类的内容，主要是可以让技术好奇者豁然开朗的细节。

就像互联网上日新月异的各种技术一样，区块链技术也是一项正在风口浪尖上的创新技术。只有不断学习、跟踪、了解、把握这些新技术，才能不被后浪拍在沙滩上。

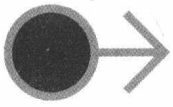
编　者

2019 年 4 月

教学建议


【研究生、本科生课程】
全面和细致掌握(40～60学时)
【短训课程】
技术细节和技术发展(16～20学时)
【研修课程】
技术原理和典型应用(8～10学时)
【专题讲座】
选题相关内容(2～4学时)
第1章 货币认知
第2章 比特币认知
第3章 密码学基础
第4章 数字签名技术
第5章 对等网络技术
第6章 比特币技术原理
第7章 比特币应用体系
第8章 区块链技术原理
第9章 区块链技术演进
第10章 区块链安全威胁
第11章 区块链安全防范
第12章 区块链技术应用

目录



第1章　货币认知

“有钱，还是没钱，这是一个问题。”

听到 Alice 忽然冒出这么一句，正在埋头看一段软件代码的 Bob 觉得莫名其妙。“你是莎士比亚看多了，还是想着买新衣服？”别看 Bob 愣头愣脑的，看问题却挺“深刻”。

Alice 白了他一眼，合上读了一小半的书，若有所思地喃喃自语：“钱究竟是什么？钱从何而来？我能不能‘造’钱呢？”

“别！那犯法！”Bob 快速脑补了 Alice 在自制印钞机前刷刷地印伪钞然后被人赃俱获带走的惨状。

“合法的货币是国家发行的。”Alice 继续自己的思索，“但从来如此吗？永远如此吗？”“呃……”Bob 的大脑门上瞬间多了几条黑线。

Alice 解释道：“虚拟币被炒得火热，我很好奇它是怎么运作的，但我得先搞清楚货币究竟是什么！”

1.1　货币简史

Alice 穿越到了上古时代。

“你这毛皮多少钱？”Alice 问胡子拉碴的猎人，他长得酷似 Bob。“啥？啥是钱？”猎人 Bob 一脸不屑的样子，骄傲地说：“我这可是最上等的皮子！除非拿你养的一头羊才能换！”

Alice 瞬间明白了，她用力过猛，回到了七八千年前，那还是个物物交换的远古时代，怪不得猎人完全不知道钱为何物。一定是穿越计数器不小心多按了一两个零。

当古代人类基本上满足了温饱需求后，自然会想到用富余的猎物、家畜、稻米、工具去跟别人换取自己所缺少的东西，满足多样化的日常需要。例如，渔夫需要农家的大米，猎人需要山民的竹子。这就开启了以物易物的进程，商品出现了，甚至还出现了市场，从此一发而不可收。人们渐渐意识到：只要有能力生产更多的东西，就能换取更多的商品，生活就能过得更美好。

在商品交换过程中，逐步形成了价值的概念。不同的东西具有不同的价值，通常越稀有、越难获取的东西价值越高。会干活的马当然比好吃懒做的猪贵，一匹马可以轻轻松松换三头猪；狩猎工具需要能工巧匠才能做出来，要拿一头鹿加两只野鸡来换。

但是以物易物制存在两个突出矛盾：一是 Alice 想换 Bob 的毛皮，但 Bob 不想要 Alice 养的羊，他们的交易就没法达成；二是 Bob 不想一次性换来一大堆东西，照管都不方便，还影响自己四处迁移打猎。四肢发达、头脑灵活的 Bob 在篝火上边烤野味边突发奇想：假如有“一样东西”，我打了猎物先换成“这样东西”，等我需要的时候可以拿“这样东西”换别人的刀和箭，这该多好啊！

Bob 畅想的“这样东西”应该具有这些属性：首先要得到公认，大家都遵守公平交易的规则；其次能代表一定的价值，且保持相对恒定，例如多少数量可以换一头羊；还有应不易获得，否则就会乱套；最后需要比较便携，可以轻松揣在口袋里随掏随用。有了“这样东西”，人与人之间的交易活动就能拆分为“卖”和“买”两种相互独立的行为，这样就放松了时间、空间、需求等约束，使交易更灵活，生产者积极性大增，财富也更容易积累。“这样东西”就是货币(currency)。

> 现代的电脑迷 Bob 会这样点评他祖先的创新思想：“就是把同步会话过程异步化了，有效降低了两者间的耦合度，可极大地提升业务并发能力。”他可不管自己的点评反而让别人云里雾里。

可喜的是，大约从四千年前开始，古人 Bob 的理想终于实现了。

生活在华夏大地上的先民是使用“钱”最早的族群之一。如图 1.1 所示，当时的人们用的是天然海贝(sea shell)。酷爱海鲜的吃货们有理由为此心花怒放，因为吃的是美味的贝肉，吐出来的都是“钱”啊！海贝要符合上述货币属性，恐怕这就是唯一的疑问：这货太多了，不是很容易泛滥成灾吗？

倘若 Alice 把穿越计数器调准，来到那个货币刚刚诞生的年代，她就会发现有人聚居的地方一般都在内陆，在水草肥美的平原或山地，那时人类还没有足够的能力征服狂野

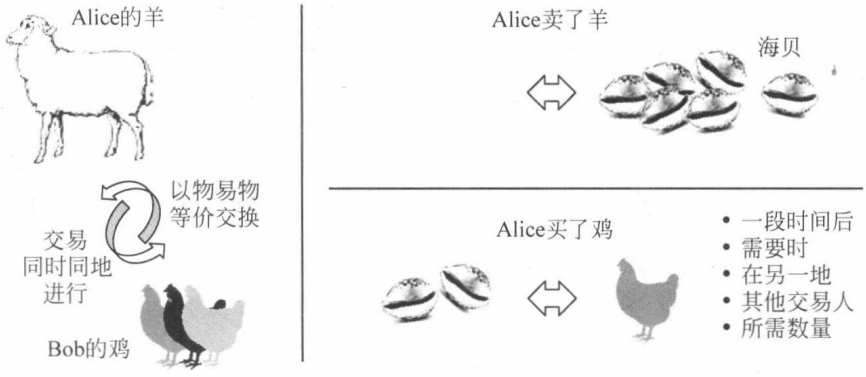


图 1.1　从以物易物到等价物交换示意图

的大海。因此，身在此时此地，天然海贝就是稀罕之物。人们要采到海贝，需要付出翻山越岭、劈风斩浪的巨大代价，就像通过开矿、淘沙、冶炼来得到金子一样。虽然采贝人没有种稻、养羊，但是他们付出的工作量是得到认可的，他们可以用海贝来换取商品，而海贝也由此以“钱”的身份进入流通领域。

掂量着手里几枚“身价不菲”的海贝，穿越而来的 Alice 若有所悟：货币其实是人们的一种约定，是用来做交易的中间媒介；此时只有群落和部落，“国家”还没出现呢，所以货币完全是产生于民间、流通于民间的。

现代经济学家把货币定义为“一般等价物”，本质上是所有者之间关于交换权的契约。正因为货币与价值挂钩，其发行数量应当与商品生产总量相当，才能保证货币体系的稳定，否则就会导致通货膨胀或通货紧缩。设想有一天，英俊的采贝人 Bob 在海边与美人鱼相遇相爱，美人鱼给 Bob 带来数不清的海贝，Bob 一夜暴富，建起了面朝大海的豪华别墅，而市场上的海贝成倍地增多，因此越来越贬值，于是原来几个海贝可以换一头羊，现在 500 个都不够了。幸运的 Bob 无意间就可能触发了人类史上第一次通货膨胀。

Alice 继续在时空隧道里跳跃。大地还是这片大地，却转眼间沧海桑田、物是人非，Alice 一路看到了各式各样的钱：黄帝时代出现了金属货币，称为铜仿贝、钱镈(布)；商周时代金属货币大量通行；春秋时期出现了刀币、方孔圆钱(俗称“孔方兄”，指代钱，也是很多现代中国银行标识设计的来源)；战国时期开始流通黄金；东汉首次用铁来铸币；汉代以黄金为上币、铜钱为下币；宋代出现了交子，为局部地区使用的纸质信用凭证，可以用来兑换钱；到了元代纸币正式登上历史舞台，不铸铜币，只用纸钞，这标志着货币实现

了彻底的符号化。

自从国家出现以后，作为主权象征，也是掌控国家经济命脉的需要，货币都由国家政府来铸造（印制）和发行，这就是法定货币（简称法币）。通常每个国家都发行自己的法定货币，但是也有例外，例如，欧元区各国使用同一种欧元（允许有各个国家的版本）；一个国家内各个自治体可以发行不同的货币并可相互流通，如英国，但国际上只承认一种英格兰英镑；也有经济不发达小国指定别国货币作为自己的法定货币。

货币是匿名的，只有银行账号是实名的，即与持有人的真实身份相关联。由于货币可以换取财富，自古以来就一直有不法之徒不惜铤而走险，仿制法定货币以牟取暴利，各国政府因此在不断打击伪钞的同时，不断研究货币（尤其是大面值纸币）的防伪技术，增加伪造难度。显然，只要现金存在一天，这一“斗争”必然会持续下去。

1.2 数字货币

近现代资本主义经济的发展推动了金融业的繁荣，人类的财富不再是实物和货币那么简单，而是有了股票（股份）、债券、保险、外汇、期货等各种变化形态。但无论如何，法定货币依然是本源。

更大的变化来自于计算机和网络的诞生。货币逐步实现了数字化，可满足快速、远距资金流动的需要，如消费、转账、兑换等，避免了提着大量现金来回奔波的低效、不便和危险，还不易受伪钞的困扰。现代银行业发明了银行卡，包括用于资金储蓄并使用的借记卡（debit card）和可凭个人信用进行消费透支、先用后还的信用卡（credit card），实现了国际标准化，达到了在不同银行间互联互通的操作目的，消费领域开启了“无现金交易”时代。近年来，中国的移动互联网应用蓬勃发展，领全球风气之先，基于智能手机的“移动支付”功能迅速普及，从买早点、坐公交、发红包，到购买大件商品、异地跨行转账，都可仅借助一部手机扫描二维码或在网上银行、第三方支付的 APP 点击几次即可完成，连银行卡都免了，完成了到“无卡片、无现金”交易的华丽转身。

“请配合做个小调查好吗？”Alice 递给好朋友 Bob 一块巧克力，“你身边有多少钱？”

Bob 毫不客气地把巧克力塞到嘴巴里，掏出钱包，抽出几张皱巴巴的纸币和几个硬币，含糊不清地说：“43 块 8。可以请你喝咖啡。”